MALICIOUS

Classifications: Spyware

Threat Names: C2/Generic-A, AgentTesla.v3, Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe**
ID	#5067696
MD5	ba7863b67930a109864139efe3da478e
SHA1	0a90df33ba078ba54576906d6072a11b8dca5356
SHA256	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb
File Size	779.00 KB
Report Created	2022-08-05 15:02 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (24 rules, 70 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Agent Tesla configuration was extracted	1	Spyware
	• A configuration for Agent Tesla was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
	• Rule "AgentTesla_StringDecryption_v3" from ruleset "Malware" has matched on a memory dump for (process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe.			
5/5	_data_collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Flock, FTP Navigator, Internet Download Manager, Mozilla Thunderbird, Opera Mail, FileZilla, Incr... ...er, SeaMonkey, Comodo IceDragon, Postbox, Opera, OpenVPN, CoreFTP, k-Meleon, Mozilla Firefox, WinSCP, Cyberfox, Microsoft Outlook.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
4/5	Reputation	Contacts known malicious IP address	1	-
	• Reputation analysis labels the contacted IP address 208.91.198.143 as C2/Generic-A.			
2/5	Defense Evasion	Sends control codes to connected devices	3	-
	• (Process #4) wmiprvse.exe controls device "\\.\{9E8A7ED5-49C8-421B-A782-D46C28931105}" through API DeviceIOControl. • (Process #4) wmiprvse.exe controls device "\\.\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}" through API DeviceIOControl. • (Process #4) wmiprvse.exe controls device "\\.\{E96D977E-F067-4CE9-924D-F6E0A04729E4}" through API DeviceIOControl.			
2/5	_data_collection	Reads sensitive browser data	9	-
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of web browser "Opera" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of web browser "BlackHawk" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of web browser "Flock" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of web browser "k-Meleon" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of web browser "Comodo IceDragon" by file.			
2/5	_data_collection	Reads sensitive mail data	7	-
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of mail application "The Bat!" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of mail application "IncrediMail" by registry. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of mail application "Postbox" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of mail application "Opera Mail" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of mail application "Pocomail" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	_data_collection	Reads sensitive application data	6	-

Score	Category	Operation	Count	Classification
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of application "WinSCP" by registry. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of application "Internet Download Manager" by registry. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of application "SeaMonkey" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of application "OpenVPN" by registry. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of application "TightVNC" by registry. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of application "TigerVNC" by registry.		
2/5	_data_collection	Reads sensitive ftp data	4	-
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of ftp application "CoreFTP" by registry. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of ftp application "Ipswitch WS_FTP" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of ftp application "FileZilla" by file. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to read sensitive data of ftp application "FTP Navigator" by file.		
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe queries OS version via WMI.			
2/5	Discovery	Executes WMI query	2	-
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe executes WMI query: select * from Win32_OperatingSystem. • (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe executes WMI query: SELECT * FROM Win32_Processor.			
2/5	Discovery	Collects hardware properties	1	-
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe queries hardware properties via WMI.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe modifies memory of (process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe alters context of (process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe starts (process #1) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe reads from (process #1) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Possibly does reconnaissance	22	-

Score	Category	Operation	Count	Classification
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "blackHawk" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "The Bat!" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "WinSCP" by registry.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "Qualcomm Eudora" by registry.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "Postbox" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "WS_FTP" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "FlashFXP" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "Opera Mail" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "icecat" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "SeaMonkey" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "Flock" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "Cyberfox" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "FileZilla" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "Pocomail" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "Mozilla Firefox" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "FTP Navigator" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "k-Meleon" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "Comodo IceDragon" by file.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "Foxmail" by registry.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "RealVNC" by registry.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "TightVNC" by registry.			
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to gather information about application "TigerVNC" by registry.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe resolves host name "us2.smtp.mailhostbox.com" to IP "208.91.199.225".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe opens an outgoing TCP connection to host "208.91.199.225:587".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe tries to connect to TCP port 587 at 208.91.199.225.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #2) 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe resolves 52 API functions by name.			

Malware Configuration: AgentTesla

Metadata	Key	Extracted Value
Email Address	Tags Value Tags Value	Sender info@szlikestechs.com Recipient info@szlikestechs.com
URL	Url Tags Username Password	us2.smtp.mailhostbox.com SMTP Server info@szlikestechs.com Logistics@1234
Encryption Key	Key Algorithm	qg== XOR

Mitre ATT&CK Matrix

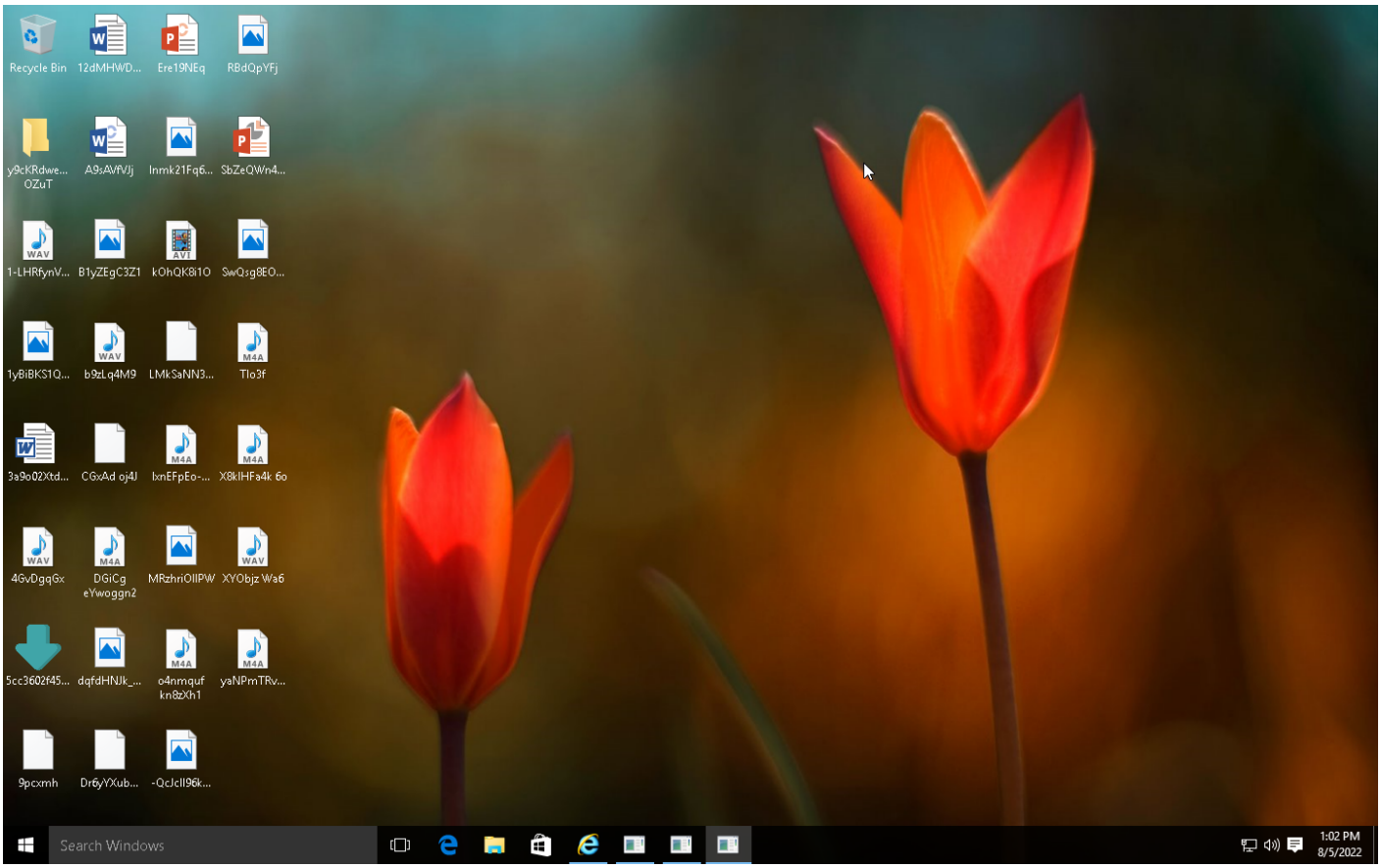
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection	#T1065 Uncommonly Used Port		
				#T1045 Software Packing	#T1214 Credentials in Registry	#T1012 Query Registry		#T1005 Data from Local System			
					#T1003 Credential Dumping	#T1082 System Information Discovery					

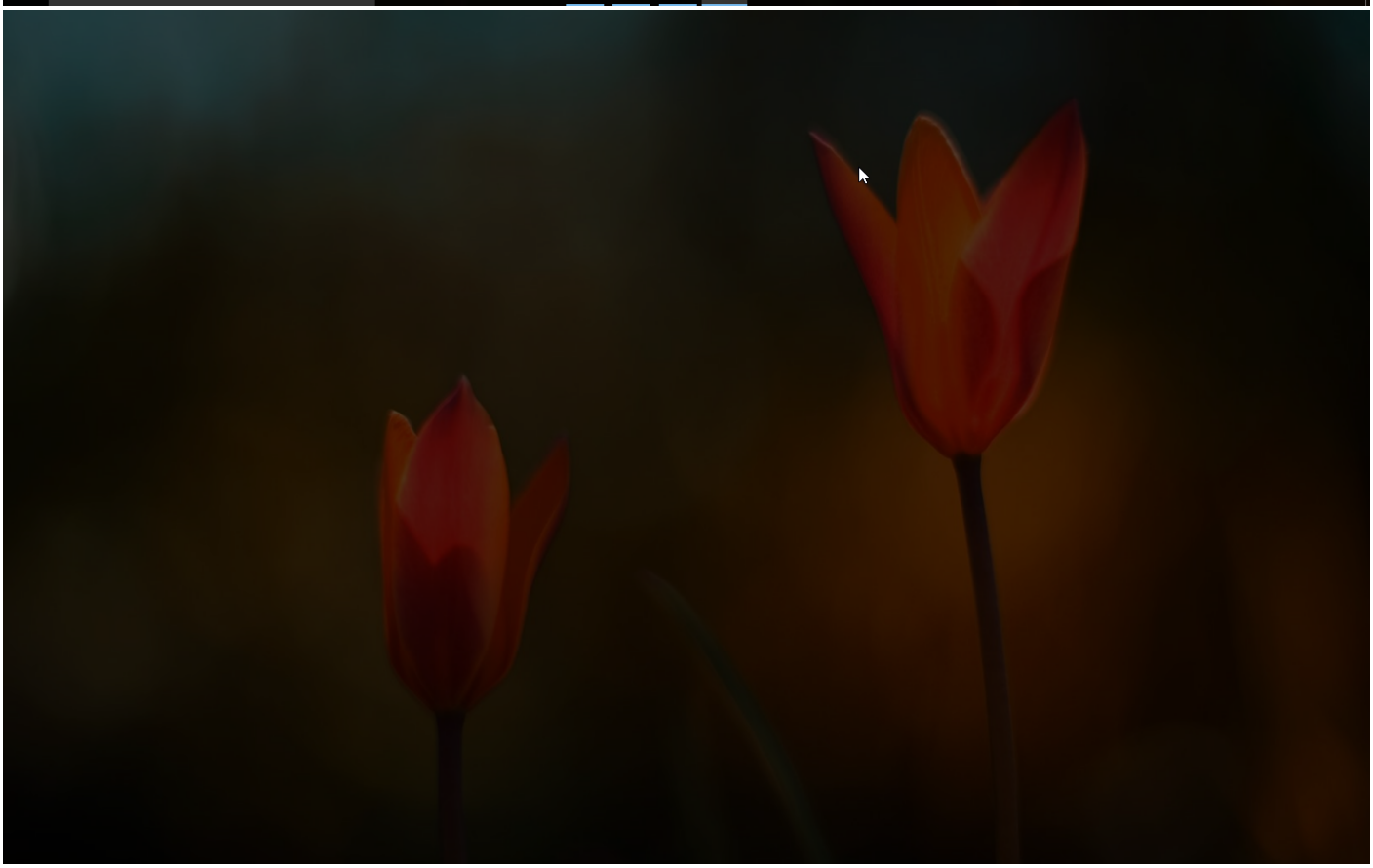
Sample Information

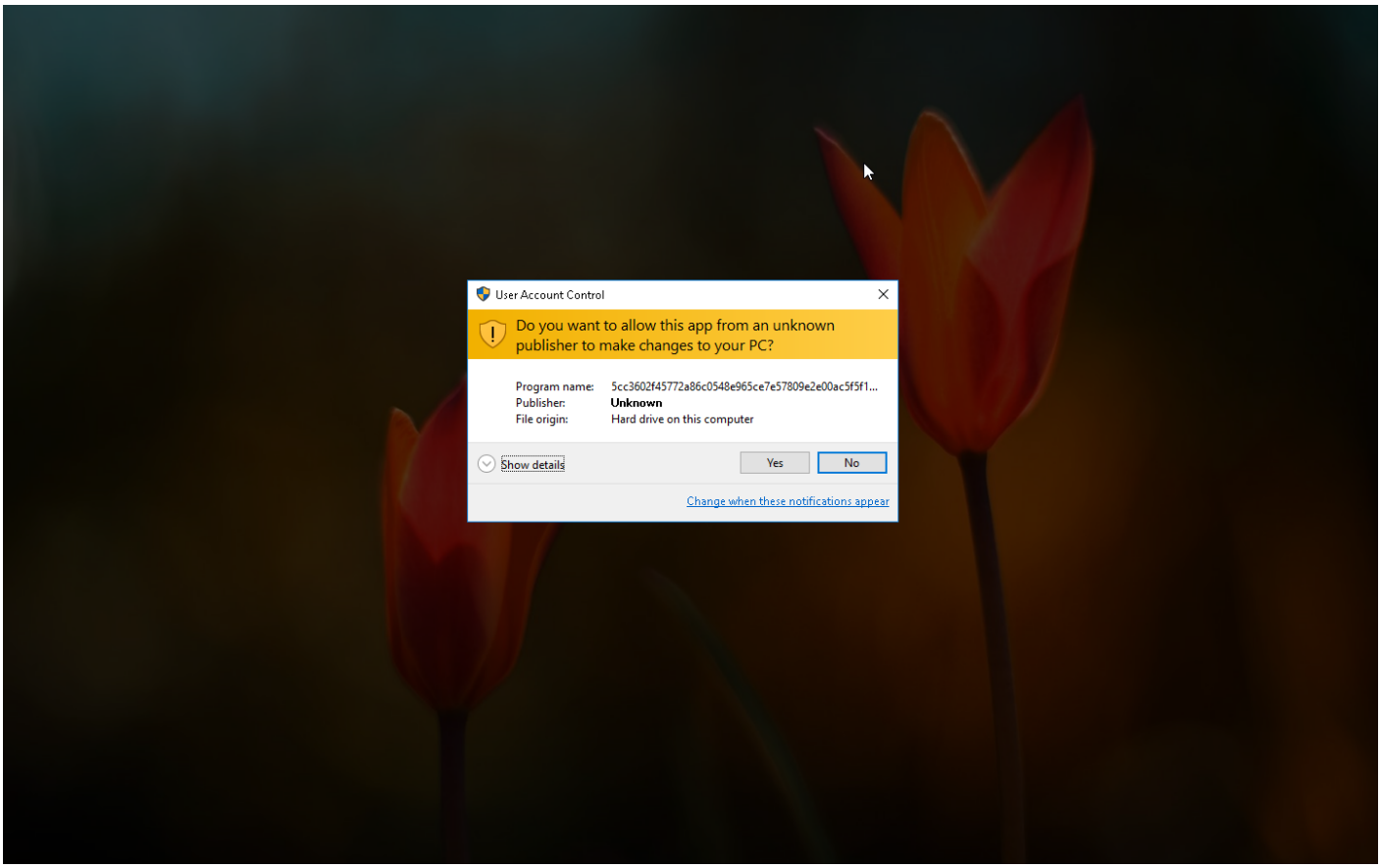
ID	#5067696
MD5	ba7863b67930a109864139efe3da478e
SHA1	0a90df33ba078ba54576906d6072a11b8dca5356
SHA256	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb
SSDeep	12288:zbv7n02b2UVFdPBGjy1AuFWBVeS5f/QBK7CNhvk0R4pRmCDqHVVAx67WeyqLvLqh:3Gjy1AuBS5c+Y7ipRmb13W4LzEkM
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe
File Size	779.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

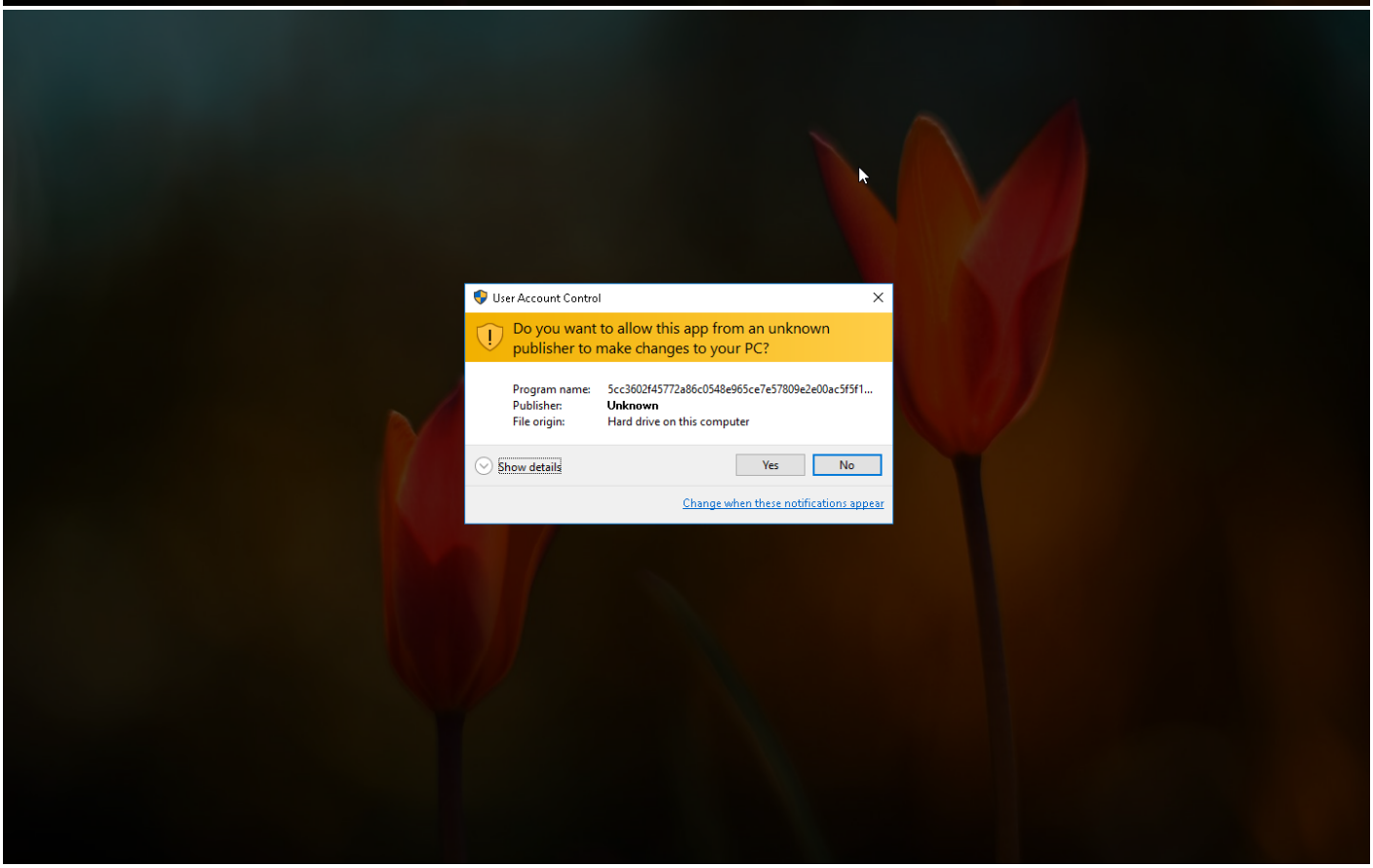
Analysis Information

Creation Time	2022-08-05 15:02 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	1


Recycle Bin
12dMHWD...
Ere19NEq
RBdQpYFj
y9cKRdwe...
OZuT
A9zAVfVJj
Inmk21Fq6...
SbZeQWn4...
1-LHRfymV...
B1yZEgC3Z1
kOhQK8i1O
SwQsg8EO...
1yBiBKS1Q...
b9zLq4M9
LMkSaNN3...
Tlo3f
3a9o02Xtd...
CGxAd oj4J
lxnEFpEo-...
X8klHFa4k 6o
4GvDgqGx
DGiCg
eYwoggn2
MRzhriOIIPW
XYObjz Wa6
5cc3602f45...
dqfdHNJk_...
o4nmquf
kn8zXh1
yaNPmTRv...
9pcxmh
Dr6yYXub...
-QcJcll96k...
Search Windows
1:02 PM
8/5/2022







Screenshots truncated

NETWORK

General

2.32 KB total sent

8.05 KB total received

2 ports 587, 53

2 contacted IP addresses

1 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

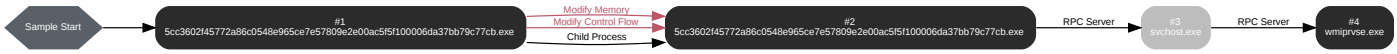
0 sessions, 0 bytes sent, 0 bytes received

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	us2.smtp.mailhostbox.com	NO_ERROR	208.91.199.225, 208.91.199.223, 208.91.199.224, 208.91.198.143		NA

BEHAVIOR

Process Graph



Process #1: 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 60734, Reason: Analysis Target
Unmonitor End Time	End Time: 164468, Reason: Terminated
Monitor duration	103.73s
Return Code	0
PID	2552
Parent PID	1972
Bitness	32 Bit

Host Behavior

Type	Count
Registry	4
Module	1142
Window	22
File	20
COM	1
System	3
Process	1
-	3
-	7

Process #2: 5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 162008, Reason: Child Process
Unmonitor End Time	End Time: 300808, Reason: Terminated by timeout
Monitor duration	138.80s
Return Code	Unknown
PID	4420
Parent PID	2552
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	0x448	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	0x448	0x402000(4202496)	0x33c00	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	0x448	0x436000(4415488)	0x600	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	0x448	0x438000(4423680)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	0x448	0x2a6008(2777096)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	0x448 / 0x115c	0x435b8e(4414350)	-	✔	1

Host Behavior

Type	Count
-	22
Registry	98
File	136
User	4
Module	67
System	31
COM	34
Environment	27

Type	Count
-	2
Mutex	2
-	1
Window	3

Network Behavior

Type	Count
DNS	1
TCP	1

Process #3: svchost.exe

ID	3
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 167830, Reason: RPC Server
Unmonitor End Time	End Time: 300808, Reason: Terminated by timeout
Monitor duration	132.98s
Return Code	Unknown
PID	864
Parent PID	4420
Bitness	64 Bit

Process #4: wmiprvse.exe

ID	4
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 167830, Reason: RPC Server
Unmonitor End Time	End Time: 300808, Reason: Terminated by timeout
Monitor duration	132.98s
Return Code	Unknown
PID	4236
Parent PID	864
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Registry	4
Module	20
File	5
-	6

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb	C:\Users\RDhJ0CNFevzX\Desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	Sample File	779.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
f67286259cf7d1c5b4f7a67a3ac6fa542d1989fc9a8ebf5ef4f208bdec8895fc	-	Extracted File	3.89 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data\Default\EncryptedStorage	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files (x86)\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Trillian\users\global\accounts.dat	Accessed File	Access	CLEAN
\\.\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Psi\profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Ipswitch\WS_FTP\Sites\ws_ftp.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\ProgramData\FlashFXP\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Claws-mail	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\profiles.ini	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\Private Internet Access\data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files\Foxmail\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\uvnc bvba\UltraVNC\ultravnc.ini	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Psi+\profiles	Accessed File	Access	CLEAN
C:\Private Internet Access\data	Accessed File	Access	CLEAN
\\.\{E25A642B-6CEB-4194-8F83-8BC82AF94F5A}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Mail\Opera Mail\wand.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Credentials\	Accessed File	Access	CLEAN
\\.\{E96D977E-F067-4CE9-924D-F6E0A04729E4}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\NordVPN	Accessed File	Access	CLEAN
C:\Program Files (x86)\jDownloader\config\database.script	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Folder.lst	Accessed File	Access	CLEAN
\\.\{9E8A7ED5-49C8-421B-A782-D46C28931105}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
C:\Storage\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FTPGetter\servers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FlashFXP\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Waterfox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\MySQL\Workbench\workbench_user_data.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHawk\profiles.ini	Accessed File	Access	CLEAN
C:\cftp\Ftplist.txt	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\FTP Navigator\Ftplist.txt	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\icecat\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data	Accessed File	Access	CLEAN
\\.\{017EF944-8C88-42C3-8F92-C8F7B6022F8D}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Mailbird\Store\Store.db	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Postbox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Flock\Browser\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\The Bat!	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\plutil.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\UltraVNC\ultravnc.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Comodo\IceDragon\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Claws-mail\clawsrc	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\RichEd20.DLL	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data	Accessed File	Access	CLEAN
C:\mail\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Pocomail\accounts.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Protect\S-1-5-21-1560258661-3990802383-1811730007-1000\1c1d304f-aa8f-4534-b2cb-33b61c83ed15	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\falkon\profiles\profiles.ini	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\eM Client	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://us2.smtp.mailhostbox.com	-	208.91.199.224, 208.91.198.143, 208.91.199.223, 208.91.199.225	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
us2.smtp.mailhostbox.com	208.91.199.224, 208.91.198.143, 208.91.199.223, 208.91.199.225	-	TCP, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
208.91.198.143	us2.smtp.mailhostbox.com	United States	DNS	MALICIOUS
208.91.199.223	us2.smtp.mailhostbox.com	United States	DNS	CLEAN
208.91.199.225	us2.smtp.mailhostbox.com	United States	TCP, DNS	CLEAN
208.91.199.224	us2.smtp.mailhostbox.com	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
-	delete, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\DownloadManager\Passwords	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TightVNC\Server	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\TigerVNC\Server	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\vncserver	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\TigerVNC\Server	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\FoxmailPreview	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\RealVNC\WinVNC4	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\vncserver	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\ORL\WinVNC3	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\RealVNC\WinVNC4	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Qualcomm\Eudora\CommandLine	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\FTPWare\COREFTP\Sites	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\TightVNC\Server	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\OpenVPN-GUI\configs	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\Software\RimArts\B2\Settings	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions	access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	CLEAN

Process

Process Name	Commandline	Verdict
5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe"	SUSPICIOUS
5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\5cc3602f45772a86c0548e965ce7e57809e2e00ac5f5f100006da37bb79c77cb.exe"	SUSPICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	AgentTesla_StringDecryption_v3	Agent Tesla v3 string decryption	Memory Dump	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.14 / 2022-08-03 12:19:21
YARA Built-in Ruleset Version	4.6.1.10

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp

System Root	C:\Windows